22. (Amended) A system comprising:

a first system for issuing scrip, the scrip including a value derived from an identification of a recipient of the scrip; and

a second system for receiving the scrip issued by the first system from a party seeking a refund and issuing a refund in response thereto, the second system further adapted to receive from the party seeking the refund the identification of the recipient of the scrip and values enabling transformation by the second system of the identification of the recipient of the scrip into the value derived from the identification of the recipient of the scrip, and to utilize the received values to verify that the party seeking the refund is the recipient of the scrip.

B5

## REMARKS

Claims 3-6, 11-17, and 19-22 were pending and rejected. Applicants have amended claims 6, 11, 12, 15, and 22. Claims 3-6, 11-17, and 19-22 remain pending.

Claims 6, 12, and 15 have been amended to conform with their parent claims. The amendments to claims 6 and 12 do not narrow their scope.

Claims 3-6, 11-17 and 19-22 stand rejected under 35 U.S.C. § 103 (a) as being anticipated by Hiroya et al. (EP 0848 343 A2) in view of Chaum (US Pat No. 5,373,558) and Manasse (US Pat. No. 5,802,497). In response, independent claims 11 and 22 have been amended to recite features similar to independent claim 17. Claim 17 recites:

17. A computer readable medium having computer instructions encoded thereon for directing a computer system to provide a refund in an electronic commerce system, the computer instructions comprising instructions for:

receiving a request to refund electronic currency, the electronic currency including a value identifying the party to whom the currency was issued;

receiving, from the party seeking the refund, identifying information identifying the party seeking the refund and **values for transforming the information identifying the party seeking the refund into the value identifying the party to whom the currency was issued;**

utilizing the received values to verify that the received identifying information matches the value in the electronic currency identifying the party to whom the electronic currency was issued; and

responsive to a positive verification, entitling the party to whom the electronic currency was issued to a refund for the electronic currency.

Thus, claim 17 recites receiving, from the party seeking the refund, values for transforming identifying information into a value in the currency. As the identifying information and the values for transforming are both provided by the party seeking the refund, these features enable the system to identify a party involved in an anonymous transaction without necessarily referencing a third party key or external means of verification. Claims 11 and 22, as amended, recite these receiving and transforming steps.

As previously discussed, Hiroya discloses an electronic shopping system. In Hiroya's system, however, the party seeking the refund supplies only the repayment permit, the digital signature, and the digital certificate. The electronic money payment server must contact the certificate authority in order to derive the Repayment Recipient ID from the digital signature. Without the certificate authority, Hiroya has no way to authenticate the party seeking the refund.

Therefore, Hiroya's system does not receive the values for transforming the information identifying the party seeking the refund from the party seeking the refund, as claimed. Instead, Hiroya's system receives these values from a certificate authority.

Furthermore, this distinction was directed to the Examiner in Applicants' response to the Office Action dated April 9, 2001. The most recent Office Action does not address this issue and, in fact, skips over this feature of claim 17 without mention.

Chaum similarly does not disclose or suggest a system whereby a party seeking to identify itself provides all of the information necessary for its identification. Chaum discloses a system whereby a signer submits a signature with two parts. The first part of the signature is self authenticating, the second part can only be authenticated by referencing a public key held by a third party confirmation system. Thus, unlike the system recited in claim 17 and amended claims 11 and 22, the recipient in Chaum cannot verify the identity of another party without contacting a third party key.

The examiner acknowledges that Manasse does not disclose a mechanism for providing refunds. Accordingly, Applicants respectfully submit that a person of ordinary skill in the art would not find it obvious to receive the values for transforming from the party seeking the refund as claimed in view of Hiroya, Chaum, and Manasse, either alone or in combination. For this reason, Applicants respectfully submit that claims 11, 17, and 22 are allowable over the prior art.

Claim 19 recites the features of claim 17 and further recites:

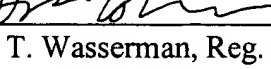
> receiving one or more nonces with which the information identifying the party seeking the refund is hashed to produce the value identifying the party to whom the currency was issued.

Claim 19 recites that the values for transforming are one or more nonces. In rejecting claim 19, the Examiner cites a section of Hiroya where a data block is hashed by a private key to produce a digital signature. However, the section cited describes a digital signature provided by another server held by the party providing the refund. As the system in Hiroya discloses hashing data received from another internal server, rather than a party seeking a refund, it would not be obvious to one skilled in the art to hash data provided by the party seeking a refund, as claimed.

Claims not specifically discussed above are believed allowable by virtue of including the features of their respective base claims. Therefore, Applicants respectfully submit that the application is in condition for allowance and request that it be passed to issue. The Examiner is invited to contact the undersigned by telephone to discuss the arguments raised herein or any other aspects of the application.

Respectfully submitted,
STEVEN C. GLASSMAN *et al.*

Dated: December 19, 2001

By: 

Bryon T. Wasserman, Reg. No. 48,404
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Tel.: (415) 875-2316
Fax: (415) 281-1350

## VERSION SHOWING CHANGES MADE

6. (Amended) The system of claim 5, wherein the received [information identifying] identification of the recipient of the scrip is a hash of identifying information with a second nonce.

11. (Amended) A method of providing a refund in an electronic commerce system, comprising the steps of:

receiving, by a second party from a first party, electronic currency for which the first party seeks a refund, wherein the electronic currency includes a first value derived from information identifying the first party and wherein the second party is unable to identify the first party with the first value;

receiving, by the second party from the first party, the information identifying the first party and [instructions for deriving the first value from the identifying information] values for transforming the information identifying the first party into the first value;

using, by the second party, the [instructions for deriving the first value from the identifying information to derive a second value from the provided information identifying the first party] values for transforming the information identifying the first party into the first value to transform the information identifying the first party into a second value;

comparing, by the second party, the second value with the first value; and

enabling, by the second party, a refund for the electronic currency if the first value matches the second value.

12. (Amended) The method of claim 11, wherein the step of receiving the information identifying the first party and [instructions for deriving the first value from the identifying information] values for transforming the information identifying the first party into the first value comprises the steps of:

receiving, by the second party, information uniquely identifying the first party; and

receiving, by second party, at least one nonce with which the information uniquely identifying the first party is hashed to produce the second value.

15. (Amended) The method of claim 11, further comprising the step[s] of:
issuing, by the second party to the first party, a refund coupon entitling the first party to a refund for the electronic currency.

22. (Amended) A system comprising:
a first system for issuing scrip, the scrip including a value derived from an identification of a recipient of the scrip; and
a second system for receiving the scrip issued by the first system from a party seeking a refund and issuing a refund in response thereto, the second system further adapted to receive from the party seeking the refund the identification of the recipient of the scrip and [information] values enabling transformation by the second system of the identification of the recipient of the scrip into the value derived from the identification of the recipient of the scrip, and to utilize the received [information] values to verify that the party seeking the refund is the recipient of the scrip.